Removable Security Device (Smartcard)

Product Evaluation Summary

Smart Card Reader, USB Security Token, PC USB SIM Card, USB Integrated Chip Card (UICC)

September 2003

Revision 1.2

1 Wireless connectivity and some features may require you to purchase additional software, services or external hardware. Availability of public wireless LAN access points limited. System performance measured by MobileMark* 2002. System performance, battery life, wireless performance and functionality will vary depending on your specific hardware and software configurations. See http://www.intel.com/products/centrino/more_info for more information.

Contents

Figures and Tables

Revision History

Rev.	Description	Date
1.00	Initial Release	December 2002
1.1	Add compliant product to list	March 2003
1.2	Add compliant product to list	September 2003

Abstract

Protecting data for personal computer users is critical and coming more into focus as the number of mobile PC users increase, data security attacks intensify, and data theft becomes more common. Hardware removable security devices such as smart cards, USB security tokens, and other similar device classes can provide the foundation for improved data security. Care should be taken in the design and implementation of these security devices to ensure proper function without adversely impacting the notebook computer use. This document provides a simple set of evaluation guidelines along with a summary of products assessed using these guidelines.

1. Introduction

Platform security is critical to ensure the trust and confidence users have for keeping their own data and sensitive third party data safe both within the computer as well as when it may be transmitted across a communications channel to another user. The need to protect data and secrets is prevalent in wired communications on corporate networks and Internet traffic, and amplified in a wireless communications environment where data is prone to additional threats. Furthermore, as the mobility of the computer platform increases, the notebook itself becomes more and more susceptible to theft. Safer computing is a necessity in moving the computer industry forward and is complimentary to the pillars of mobile next generation notebook PCs defined by Intel.

This document provides an outline for testing criteria useful in evaluating removable security device categories including smart card readers, USB security tokens, PC SIM Card readers, and USB Integrated Chip Card readers for use with notebook computers. The objective of this Intel evaluation program for removable security devices is to identify products that function according to guidelines defined for use with Intel architecture-based notebook PCs. Testing has been done on several products and the results of those devices who meet these expectations are published herein. Testing was done according to the guidelines summarized in this document as executed on an Intel designed and developed customer reference system based on the Intel® Pentium® M processor.

This document and the testing results it summarizes makes no attempt to duplicate or supercede definitions and testing provided by other industry standards bodies. The guidelines provided along with the rundown for testing of removable security devices are complimentary to other standards definitions and testing methods.

Notebook PCs will progressively build on various security primitives to ultimately deliver “Trusted Client” capability for safe computing. This document summarizes guidelines defined by Intel for “removable security devices” such as smart card readers, USB security token, PC SIM card readers, USB Integrated Chip Card readers. Furthermore, a summary list of device that have been tested and shown to meet these guidelines is included herein. Other products may meet these criteria, but haven’t been tested as yet.

The intended audience of this document includes technical evaluation engineers and decision makers who will propose use of such removable security devices deployed with notebook PCs, notebook PC OEMs, as well as corporate IT planners and implementers.

Due to the variations of system design choices and security requirements, all evaluations for these products should be done independently to make sure that these products meet the specific needs of an organization. OEMs and other readers of this document should rely on their own evaluation to make the final purchase decision. Products listed within this document are not Intel products, but rather come from independent vendors and such vendors will provide their own defined warranty and support for their products. Intel does not take responsibility and provides no expressed or implied warrantees for actions or results from use of removable security device products.

Platform Security Vision

In a notebook platform, a foundation is necessary to provide secure connections for a variety of usage models. Not only must there be a method to authenticate the user for system and network logon, but also to authenticate the platform for network access. User and platform authentication relies heavily on a mechanism of the PC to securely store certificates and keys required to authenticate and ultimately protect connections and transactions.

In a roaming environment where a notebook PC may move from one connection mechanism to another, it is necessary to know the identity of the machine or person requesting access and service. Similarly, in the corporate environment it is desirable to know the identity of the machine, as well as the identity of the user requesting access and service. In both cases, authentication must occur to protect the network from unauthorized use or access. Therefore, both platform identification and user identification are desirable. Each identification mechanism provides useful information for the network provider. Platform identification allows the network to recognize the owner of the platform and the software running on it. User identification allows the network provider to discover who is requesting access. Combined, these two devices provide an enhanced level of security and authentication. Individually, each may provide enough information for a network provider to grant access to the network and certain capabilities.

For a robust solution, each of these identification mechanisms requires a hardware security device to provide the identification and the security functions needed.

The mobile platform security focus using removable security devices is intended to improve the integrity of trusted notebook PCs being marketed today as well as in the future. For those notebook platforms that are unable to incorporate the use of a fixed, motherboard security device (Trusted Platform Module or TPM), removable security devices can provide enhanced platform trust along with focused user authentication. Usage models can be supplemented with the use of a removable security device. Removable security devices can also enhance platform security used with systems that do include a fixed, motherboard security device by providing multi-factor authentication and storage of user secrets. This strategy provides the following benefits:

- Enhance existing security interfaces (e.g. Microsoft* CAPI or PKCS#11) through the hardware key generation and storage capabilities of the security device

- Potentially enhance the security features provided by user authentication, platform authentication, encrypted file system, wireless and wired connections, VPN, and other computer functions
- Provide multi-factor authentication mechanisms

All hardware security mechanisms used to enhance the ability to protect user data must perform its intended function without causing confusion to the user and without compromising battery life when used with the notebook PC. Software installation should be simple and easy to understand. This will help any potential installation done by the end user as well as streamlining the process for corporate IT. Battery life of the notebook PC remains a high priority for all mobile users, and steps should be taken by device vendors to ensure no adverse battery use impact occurs stemming from use of such security devices.

2. Intel® Centrino™ Mobile Technology Overview

Intel introduces the next step in wireless computing a reality: Intel Centrino mobile technology. Intel's breakthrough Intel® Centrino™ mobile technology goes beyond the processor to enable wireless LAN connectivity and extended battery life in the lightest, easy to carry PC designs—with outstanding mobile performance and reliability. More than just a processor, Intel® Centrino™ mobile technology contains optimized and extensively validated mobile technologies that deliver an outstanding mobile experience. Each of the components (CPU, chipset, wireless) are designed, tested and tuned by Intel to maximize the wireless mobile computing experience:

- Intel® Pentium® M processor
- Intel® 855 chipset family
- Intel® PRO/Wireless 2100 Network Connection

Intel is continuing its extensive security validation and comprehensive infrastructure verification on Intel® Centrino™ mobile technology with:

- Industry standard security and leading third party security solutions
- Wireless LAN infrastructure
- Public wireless LAN service providers

Solutions are available today that meet the needs for public, enterprise, and consumer wireless LAN deployments. Intel® Centrino™ mobile technology supports a wide range of industry security standards and leading third party solutions now and in the future.

With the focus on high performance with lower power consumption, mobile workers continue to need mechanisms to keep data secure on the notebook as well as data transmitted across any communication link. Such new generation mobile workers are increasingly dependent on wireless LAN connections where robust and reliable data protection is absolutely necessary. Data protection methods supported by the Intel Centrino mobile technology provide robust security for the increasing demands for today's mobile customers.

Mobile PCs are as different as the people who use them. That's why notebook manufacturers work hard to build products in form factors that are tailor-made for different users. Although

each mobile user may have a different way the notebook is used, data security is always a common principle for all. In an effort to encourage improvements in security solutions for mobile users, Intel has defined product guidelines and initiated hardware removable security device product evaluation with Intel Centrino mobile technology reference systems. The removable security devices summarized in this document have been tested on Intel Centrino mobile technology-based development platforms.

3. Smart Cards, USB Security Tokens: Security Solutions

This document is provided as a summary of products tested against product guidelines for removable security device (smart card, USB security token, PC SIM card, USB Integrated Chip Card) functions used with mobile PC platforms based on Intel's mobile processors and chipsets. These product categories provide additional data protection mechanisms, each bearing a different form factor with some differences in functionality.

These removable security devices take on a wide variety of sizes, form factors, functions, and intended uses. Among the most common within the category of removable security devices is the smart card. Relatively new form factors for related function devices includes USB security tokens, USB SIM cards, and USB Integrated Chip Card (UICC). All removable security devices offer "multi factor authentication": *something you have* (the device) and *something you know* (the PIN to unlock secrets stored on the device). These devices are capable of storing authentication certificates used to access computers and networks, but can only be accessed when the user enters his PIN to release that information from the device.

There are a variety of security issues that are improved through the use of hardware security devices where secrets can be safely stored and revealed only for authentication purposes. Authentication is required for both wired and more critically in a wireless environment for purposes of security and network access. In a roaming environment, it is necessary to know the identity of the machine or person requesting access and service. In the corporate environment, it is desirable to know the identity of both. In either case, authentication is essential in order to protect the network from unauthorized use or access.

Both platform identification and user identification are desirable. Each mechanism provides useful information for the network provider. Platform identification allows the network to ascertain the owner of the platform and the software running on it. User identification allows the network provider to identify who is requesting access. Combined, these two identification mechanisms provide an enhanced level of security and authentication. Individually, each may provide enough information for a network provider to grant access to the network and certain capabilities.

Each of these identification mechanisms can be implemented with a hardware token device, which provides the necessary identification and security functions. Platform identification can be protected via a Trusted Platform Module (TPM) integrated hardware token. Personal identification can be provided through a smart card or USB security token device.

Removable security devices include support to store such authentication keys along with private keys used for encryption of wireless data transmissions. The alternative to using hardware security devices to store secrets is to use the "certificate store" supported by the Windows* operating system. Implementation for Windows* 2000 and Windows XP*, this certificate store

is found in a file folder on the default hard disk. In this storage location, these certificates stored as files have no protection from theft or other virus attack.

Use of removable hardware security devices can safely store secrets used for user authentication. For example, Windows XP* has built-in support for 802.1X to improve the user authentication process for wired and wireless network connections. The Windows XP* implementation further enhances this mechanism by providing support to store and retrieve authentication certificates in removable security devices such as smart cards or USB security tokens. In fact, any hardware security device can be used to store such authentication certificates as long as that device has a compliant MS-CAPI software interface.

In general terms, all removable security devices interface to application software through standard APIs including MS-CAPI and PKCS#11. A specific layered software stack may also be defined as general purpose method of communicating to the hardware, such as the PC/SC (PC Smart Card) interface. All such industry standard software interfaces to the hardware are provided by the hardware vendor.

Smart Card Reader

A "smart card" (shown in Figure 1) is a plastic credit card size device with a built-in microprocessor and memory used to store secrets used for identification or financial transactions. When inserted into a smart card reader such as those shown in Figure 2, it transfers data to and from a notebook PC.

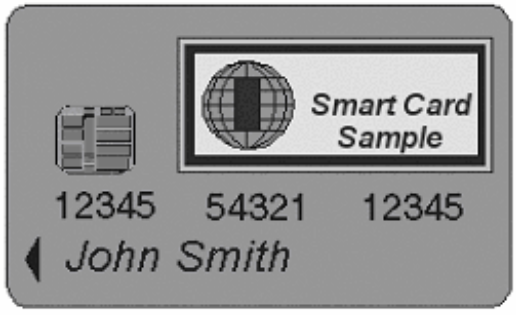

Figure 1: Smart card

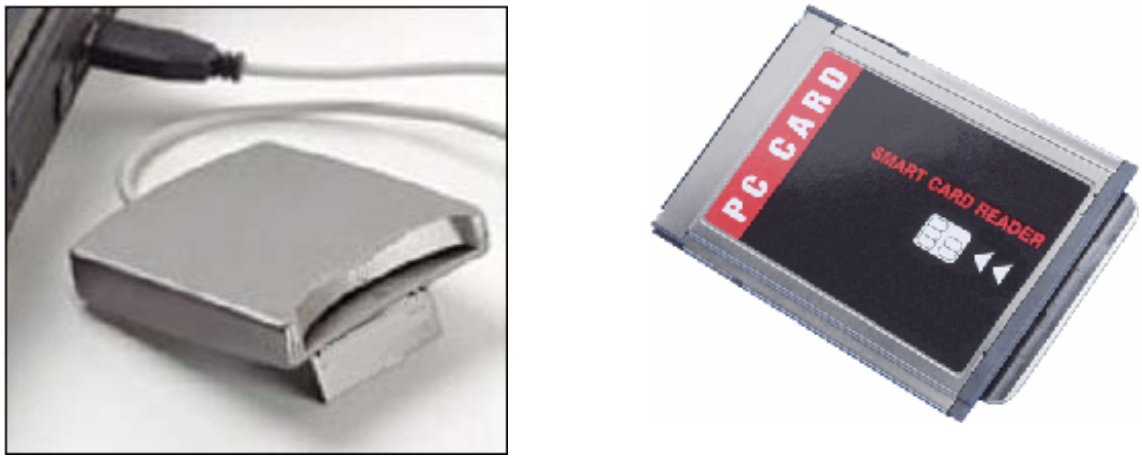

Figure 2: Smart Card Readers (USB Connection, PCMCIA Connection)

Smart cards provide enhanced security functions when plugged into a notebook PC through a smart card reader. Organizations and corporations using PCs for business and communication can take advantage of a smart card for its security functions to store important data and for its encryption capabilities. Smart cards can make private information readily available to those who need it, while at the same time protecting the privacy of individuals and keeping their informational assets safe from hacking and other unwanted intrusions. In this capacity, smart cards enable:

- Secure logon and authentication of users to PCs, wired networks, and wireless networks
- Secure B2B (business to business) and B2C (business to consumer) e-commerce
- Storage of digital certificates, credentials, passwords, and other secrets
- Encryption of sensitive data

The key advantage of using a smart card for PC security is that it provides protected storage for valuable information such as private keys, account numbers, passwords, personal information, and certificates used for authentication. Information stored on a smart card is only released upon user approval, generally in the form of a dialog box that prompts for a PIN to access smart card data. If the user enters an invalid PIN, the smart card can be pre-configured to deny all subsequent access.

The smart card is also a secure place to perform processes that shouldn't be done "exposed to the world," for example, performing a public key encryption or private key decryption. Encryption keys can be generated by the smart card with the private key stored permanently on the smart card. The private key can be used for encryption and hashing functions without ever being released from the smart card into the host operating system where it could be compromised or stolen. This is an additional benefit over existing software only security solutions.

Smart card readers attach to the notebook PC via either USB or PCMCIA and come in a wide variety of form factors and price ranges. Both smart cards and smart card readers are available from many vendors.

USB Security Token

For applications that need a form factor different than a smart card, the same functionality of a smart card is also offered on devices generically referred to as "USB security tokens" or "Smart tokens". This class of device offers user authentication, digital signatures, and data privacy all in a convenient key-sized token. They are technologically identical to smart cards, have a different form factor that is about the same size as a house key, and plug into the USB port of a notebook computer. The advantage of this class of device is that it does not require a separate reader – the reader and the security functions are bundled together into a key fob device. Figure 3below shows a USB Security Token with a house key for size comparison.

Figure 3: USB Security Token (with house key for size comparison)

Just as with the smart card, this class of device is a portable vault for private keys and other digital secrets which may include biometric templates, passwords, personal information, and e-cash. These devices can be up to 32Kbytes or more of protected storage in addition to supporting encryption and hashing methods similar to smart cards.

Because these devices are removable, they provide storage for information that needs to be portable and associated with the user as the user carries this device. When secure information is needed, the device is plugged into the computer's USB port for retrieval. Depending on the application and configuration, the device can then be removed from the PC.

The USB security token is capable of performing all private, public, and secret key functions within the token. When these critical operations are performed within the security token, a much higher level of information protection is achieved than can be provided by client-side software-only solutions. Just as with the smart card, the performance of the onboard security processor is small and large scale encryption and decryption within the device can be very slow. It is up to the particular application to choose whether the functions should be performed within the device or within the supporting software stack using the power of the computer's host processor.

USB SIM Card & Reader

A third form factor of removable security devices for smart card capabilities is offered through a tiny SIM-size smart card and reader. This class of removable security device offers removable cards that are the same size and shape as SIM cards compliant with the GSM 11.11 specification.

These tiny form factor cards are fully compliant with standard smart card definitions, just smaller measuring 25 x 15mm. The reader for the tiny smart cards provides a USB connection to the PC measures ~65 x 20 x 10 mm as shown in Figure 4 below.

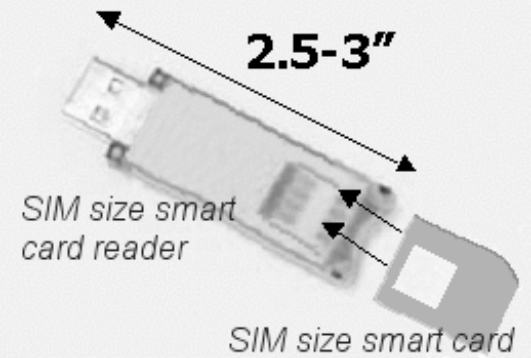

Figure 4: SIM size smart card and reader

These devices are available from several vendors to provide the same technical functionality and flexibility as a smart card or USB security token, just with a different form factor. They offer non-volatile storage and on board encryption/hashing which can be used to store private information such as user authentication certificates, passwords, and other secret data, along with the private keys used for encrypting data.

The tiny form factor smart card that is plugged into these readers is tightly coupled once inserted into the USB reader such that it won't fall out. Some product implementations provide a mechanical latch to more securely hold the tiny smart card into the reader. The tiny smart card may be removed by reversing the mechanical latch to release the card. In many cases, the usage model may be to keep the same card in the reader at all times, and rarely remove it. Other cases may require changing the SIM card for various usage needs.

USB Integrated Chip Card (UICC)

USB Integrated Chip Card (UICC) offers the same functionality as a smart card with its associated reader with added flexibility. The reader for this type of device provides a passive "pass through" for the USB connection. All USB functions are bundled onto the card itself along with the smart card functions. When the reader is plugged into a PC, it is not detected because that USB detection logic resides on the card itself. When the card is inserted into the reader, the PC then recognizes the device.

UICC cards can be implemented in two sizes: the same form factor as SIM cards and also in the same full size smart card form factor. The reader can be in a small form factor similar to the USB security token to accommodate the small SIM card or the reader can be a full size form factor to accommodate the full size smart card.

Figure 5 below represents the USB Integrated Chip Card (UICC). The outlined area of the card can be manufactured with perforations so the SIM form factor can be punched out and used in a different reader.

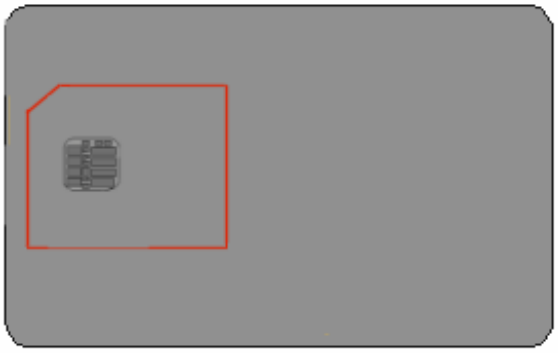

Figure 5: USB Integrated Chip Card (UICC)

4. Device Guidelines

Devices are expected to meet the following guidelines as identified by device class. Each step of this evaluation process was done with removable security products on the same platform and in the same manner defined in section 5 of this document.

Requirement	PCMCIA Smart Card Reader	USB Smart Card Reader	USB Security Token	USB SIM Card Reader
1. Device connection either via USB or PCMCIA	√	√	√	√
2. Device software installation occurs without requiring system reboot.	√	√	√	√
3. Does not block notebook system from entering Standby and is functional after system Standby and Resume.	√	√	√	√
4. Device allows host processor to enter C3 state (supports Selective Suspend) for Windows XP.	√	√	√	√
5. Each device is expected to support at least D0 and D3 ACPI power states	√	√	√	√
6. Device functions in Windows 2000, Windows XP, Windows XP-SP1, and Windows .NET Server.	√	√	√	√

Requirement	PCMCIA Smart Card Reader	USB Smart Card Reader	USB Security Token	USB SIM Card Reader
7. Device drivers WHQL certified by Microsoft.	√	√	√	√
8. Software delivered on CDROM provides INF in root directory and/or provides a simple setup utility for software installation.	√	√	√	√
9. Software installation should be simple with any user interface provided containing easy to understand instructions.	√	√	√	√
10. Provides mechanism to uninstall software support through Control Panel "Add/Remove Software"	√	√	√	√
11. Provides support for Microsoft CAPI v2.01			√	
12. Passes Microsoft CSPTESTSUITE tests for MS-CAPI CSP support			√	
13. Provides support for PKCS#11 v2.01			√	
14. Provides a software utility to read configuration information for the device.	√	√	√	√
15. Device can be store and retrieve certificates used for digitally signed email in both Windows 2000 and Windows XP without problem. Smart card readers should support this functionality using standard smart card supported within the operating system such as Gemplus, Schlumberger, or Infineon.	√	√	√	√
16. Device can be used to store and retrieve user certificates used for 802.1X authentication in Windows XP without problem. Smart card readers should support this functionality using standard	√	√	√	√

Requirement	PCMCIA Smart Card Reader	USB Smart Card Reader	USB Security Token	USB SIM Card Reader
smart card supported within the operating system such as Gemplus, Schlumberger, or Infineon.				
17. Device can be used to store user credentials used for logon used with Windows XP. Credentials should be enrolled onto the device using connection to Windows .NET server. Smart card readers should support this functionality using standard smart card supported within the operating system such as Gemplus, Schlumberger, or Infineon.	√	√	√	√

5. Evaluation Mechanics

Criteria evaluation of items listed in section 4 was done with both Microsoft Windows 2000 and Microsoft Windows XP SP1 using an Intel developed reference system. This system includes:

- Processor: Intel® Pentium®-M Processor
- Intel® 855 chipset
- Mass storage: 30GB hard drive; CD-ROM; 1.44M floppy drive
- Memory: 128MB SDRAM
- Connections: USB; PCMCIA; 10/100 Ethernet
- OS: Microsoft Windows 2000; Microsoft Windows XP SP1

This evaluation has been performed on a small sample of devices and is intended to demonstrate vendor /product capability.

For both USB and PCMCIA connection types smart card readers, testing was done using smart cards that are natively supported in Windows 2000 and Windows XP. A list of those supported smart cards is available on Microsoft's web site. At the publication of this document, operating system support includes the following:

Manufacturer	Model	Windows 2000	Windows XP
Gemplus	GemSAFE 4k	√	√
Gemplus	GemSAFE 8k	√	√
Infineon	SICRYPT v2		√
Schlumberger	Cryptoflex 4k	√	√
Schlumberger	Cyprtoflex 8k	√	√
Schlumberger	Cryptoflex Access 16k	√	√

Figure 6: Windows Supported Smart Cards

This evaluation process and the results published here are not intended to replace the normal product qualification process.

Further details of the evaluation step-by-step process are defined in a companion document titled "Removable Security Device Product Evaluation Outline" available on the Intel web site at http://developer.intel.com/design/mobile/platform/platform_collateral.htm.

6. Products Evaluation Summary

The following products listed in Table 1 perform according to the prescribed guidelines. Only products that meet the defined expectations have been included in the list below. Updates to this list with additional products will be published periodically.

It should be noted that other products may meet these guidelines, but are not included because testing has not been done.

	Vendor	**Product**
1.	Aladdin	eToken USB Security Token
2.	Axalto (formerly Schlumberger)	Reflex 20 PCMCIA smart card reader
3.	Axalto (formerly Schlumberger)	Reflex 30 PCMCIA smart card reader
4.	Gemplus	PC400 PCMCIA smart card reader
5.	Omnikey	Cardman 4000 PCMCIA smart card reader
6.	SCM Microsystems	SCR 331 USB smart card reader
7.	SCM Microsystems	SCR241 PCMCIA smart card reader
8.	Spyrus	Rosetta USB Security Token

Table 1: Vendor / Product Summary

More information for each product is listed below.

Aladdin

Vendor	**Aladdin**
Product	EToken Pro
Product Type (USB , PCMCIA)	USB Security Token
Software: Device Driver	Win2000: 01/12/2003, v3.15.0.82 WinXP: 01/12/2003, v3.15.0.82
Power Consumption	Idle: 0.2040 W Avg 0.2178 W Max Active: 0.1559 W Avg 0.2702 W Max
Vendor Contact	Daniel Pfeifle Director of National Accounts - eToken Product Line Email: Dan.Pfeifle@eAladdin.com Phone +1-847-637-4003 Fax: +1-847-818-3810 Aladdin Knowledge Systems Inc. 2920 N. Arlington Heights Rd Arlington Heights, IL 60004 Chen Arbel Vice President Support & Development Email: chen.arbel@ealaddin.com Phone: 212 329 6620 Aladdin Knowledge Systems Inc. 79 Fifth Avenue, 17th Floor New York, NY 10003 Website: http://www.ealaddin.com

Axalto

Vendor	**Axalto (formerly Schlumberger)**
Product	Reflex 20
Product Type (USB , PCMCIA)	PCMCIA Smart Card Reader
Software: Device Driver	Windows 2000: 03/08/2002, v3.6.0.1 Windows XP: 03/08/2002, v3.6.0.1
Power Consumption	Idle: 0.1054W Avg 0.1160W Max Active: 0.1660W Avg 0.2674W Max
Vendor Contact	Diane Harvey, NAM marketing manager Axalto, a Schlumberger company Phone: 1 (512) 257-3826 Mobile: 1 (512) 554 6360 Email: dmharvey@austin.sema.slb.com Website: www.axalto.com
Comments	Standard device support built into Windows 2000 and Windows XP. Driver used for testing provided by vendor.

Vendor	**Axalto (formerly Schlumberger)**
Product	Reflex 30
Product Type (USB , PCMCIA)	PCMCIA Smart Card Reader
Software: Device Driver	Windows 2000: 03/18/2002, v3.5.0.2 Windows XP: 03/18/2002, v3.5.0.2
Power Consumption	Idle: 0.0200 W Avg 0.0317 W Max Active: 0.0370 W Avg 0.0634 W Max
Vendor Contact	Diane Harvey, NAM marketing manager Axalto, a Schlumberger company Phone: 1 (512) 257-3826 Mobile: 1 (512) 554 6360 Website: www.axalto.com
Comments	Standard device support built into Windows 2000 and Windows XP. Driver used for testing downloaded from vendor website.

Gemplus

Vendor	**Gemplus**
Product	PC400
Product Type (USB , PCMCIA)	PCMCIA Smart Card Reader
Software: Device Driver	Win2000: 11/14/1999, 5.0.2183.1 WinXP: 07/01/2001, 5.1.2600.0
Power Consumption	Idle: 0.0176 W Avg 0.0317 W Max Active: 0.1178 W Avg 0.1178 W Max
Vendor Contact	Product Marketing : Jean-Marc Viande Phone : +33 442 366 926 Email: Jean-Marc.VIANDE@gemplus.com Technical support: Cedric Langlet Phone: +33 442 365 288 Email: Cedric.LANGLET@gemplus.com R&D : Frédéric Foglino Phone: +33 442 366 381 Email: Frederic.FOGLINO@gemplus.com Website: www.gemplus.com
	Support for this device bundled with Windows 2000 and Windows XP.

Omnikey

Vendor	**Omnikey**
Product	Cardman 4000
Product Type (USB , PCMCIA)	PCMCIA Smart Card Reader
Software: Device Driver	Windows 2000: 11/26/2002, v3.5.0.6 Windows XP: 11/26/2002, v3.5.0.6
Power Consumption	Idle: 0.0168 W Avg 0.0272 W Max Active: 0.0338 W Avg 0.0589 W Max
Vendor Contact	Jim Kinkead, Sales Director Phone: 1-239-642-8260 Fax: 1-239-642-8980 Mobile: 1-239-734-0000 Email: Jim@JimKinkead.com Website: www.omnikey.com
	Default driver support bundled with Windows XP. Evaluation done with updated drivers from Omnikey web site: www.omnikey.com

SCM Microsystems

Vendor	**SCM Microsystems**
Product	SCR 331 USB
Product Type (USB , PCMCIA)	USB Smart Card Reader
Software: Device Driver	Windows 2000: 10/10/2002, v4.1.01 Windows XP: 10/10/2002, v4.1.01
Power Consumption	Idle: 0.3190W Avg 0.3329W Max Active: 0.3199W Avg 0.3808W Max
Vendor Contact	Christina Cousineau, Director of Sales Phone: 1 (510) 360-2707 Mobile: 1 (408) 806-9196 Email: ccousineau@scmmicro.com Website: www.scmmicrosystems.com
Comments	None

Vendor	**SCM Microsystems**
Product	SCR 241 PCMCIA
Product Type (USB , PCMCIA)	PCMCIA Smart Card Reader
Software: Device Driver	Windows 2000: 10/22/2002, v1.04.00.01 Windows XP: 10/22/2002, v1.04.00.01
Power Consumption	Idle: 0.1751W Avg 0.1965W Max Active: 0.1983W Avg 0.2228W Max
Vendor Contact	Christina Cousineau, Director of Sales office: 1 (510) 360-2707 mobile: 1 (408) 806-9196 email: ccousineau@scmmicro.com Website: www.scmmicrosystems.com
Comments	None

Spyrus

Vendor	**Spyrus, Inc.**
Product	Rosetta USB v3
Product Type (USB , PCMCIA)	USB Security Token
Software: Device Driver	Win2000: 08/09/2003, v3.1.0.6 WinXP: 08/09/2003, v3.1.0.6
Power Consumption	Idle: 0.0044 W Avg 0.0086 W Max Active: 0.2338 W Avg 0.2789 W Max
Vendor Contact	Spyrus, Inc. **Corporate Headquarters** 2355 Oakland Road, Suite 1 San Jose, CA 95131 Telephone: (408) 953-0700 Fax: (408) 953-9835 Contact: Tom Dickens, Chief Operating Officer Tel: (408) 953-0700 Email: tdickens@spyrus.com Website: http://www.spyrus.com
Comments:	None